*Journal of Information Hiding and Multimedia Signal Processing* ©2009 ISSN 2073-4212
**Ubiquitous International** Volume **4**, Number **3**, July **2013**

# Security Analysis of Choi et al.'s Certificateless Short Signature Scheme

Yu-Chi Chen

Department of Computer Science and Engineering
National Chung Hsing University
250 Kuo Kuang Road, Taichung, 40227, Taiwan
wycchen@ieee.org

Raylin Tso

Department of Computer Science
National Chengchi University
64 Sec. 2, ZhiNan Road, Wenshan District, Taipei, 11605, Taiwan
raylin@cs.nccu.edu.tw

Gwoboa Horng

Department of Computer Science and Engineering
National Chung Hsing University
250 Kuo Kuang Road, Taichung, 40227, Taiwan
gbhorng@cs.nchu.edu.tw

Received February, 2013; revised February, 2013

Abstract. *Certificateless public key cryptography, first introduced by Al-Riyami and Paterson in 2003, is aimed to simplify the certificate management in PKI-based public key cryptography and to solve the key escrow problem of identity-based cryptography. On the other hand, Boneh et al. introduced the notion of short signatures in 2001, which are useful for systems with low bandwidth and/or low computation power. Inheriting the advantages of both certificateless cryptography and short signatures, certificateless short signatures have come into limelight in recent years. However, security and performance are always a trade-off. In 2007, Huang et al. showed security models of certificateless signature to simulate possible adversaries with their attack abilities. Recently, Choi et al. proposed a certificateless short signature scheme and showed that their scheme achieves the strongest security level. However, we have found that Choi et al.'s scheme is not as secure as they claimed. In this paper, we give comments on Choi et al. scheme including the cryptanalysis of their protocol and the weakness of their security proof.*
**Keywords:** Certificateless cryptography, Certificateless signature, Short signature, Security models, Cryptanalysis

1. **Introduction.** In traditional public key cryptography, a certificate must be provided along with a public key. The purpose of a certificate is to make sure that the public key belongs to the specific user and has not been tampered with or replaced by any third party. Those certificates are issued by a trusted authority named Certification Authority (CA). In PKI-based public key cryptography, CAs fully manage and maintain the certifications including the certificates revocation, storage, distribution and verification, etc. These tasks are generally considered costly and time consuming for CAs. However, with development of wireless networks such as ad hoc networks, communication cost is

required to decrease between users and CA. A straight solution is a cryptsystem which does not adopt CAs. Therefore, both of identity-based public key cryptography (ID-PKC) [12, 17] and certificateless public key cryptography (CL-PKC) [1] are constructed without the trusted party to manage certificates, which also simultaneously need lower communication cost. Technically, they only depend on a trusted entity to generate keys. One of the security issues of ID-PKC is the *key escrow* problem in which the trusted entity, named Private Key Generater (PKG), has every user's secret key. However, the core of CL-PKC is the trusted entity, named Key Generation Center (KGC), which cannot have the user's actual secret key. The KGC only owns user's *partial private key*, which is the most different property from ID-PKC. As a result, CL-PKC is one of the most dependable methods to avoid key escrow in practice.

Certificateless public key cryptography has attracted significant research attention since it was first introduced by Al-Riyami and Paterson in 2003. Certificateless signature (CLS) therefore becomes popular for a decade [3, 4, 5, 8, 18]. Existential unforgeability is an important issue when designing a provably secure CLS scheme. As well-known, there are two types of adversaries in CLS: one is referred to as the Type I adversary acting as an outside attacker, and the other is referred to as the Type II adversary acting as the KGC. Type I adversary can replace any user's public key, but it cannot access the system master key which is held by the KGC. Type II adversary holds the system master key, but it cannot replace public keys.

Taking the security of CLS into consideration, Huang et al. [9] in 2007 discussed the security of CLS schemes and re-defined the adversary's models in it. According to their definition, adversaries are classified into Normal, Strong, and Super adversaries which are ordered by their attack abilities. The Super adversaries are more powerful than others respectively. In addition, some certificateless short signature schemes have been proposed to provide lower communication cost [6, 7, 16], but Shim presented an attack which is performed by the Strong or Super Type I adversary against short CLS schemes [13]. In practice, to design a secure short CLS schemes withstanding this attack is an open problem. Recently, Choi et al. proposed a CLS scheme and claimed their scheme is secure against the Super Type I and II adversaries as the strongest security level [5]. In this paper, we have found Choi et al.'s short CLS scheme is not as secure as they proved. We cryptanalyze this scheme and indicate the weaknesses of the security proof. We conclude that Choi et al.'s scheme is insecure against the Strong Type I adversary. Consequently, it is also not secure against the Super Type I adversary.

The rest of this paper is organized as follows. We briefly describe preliminaries in Section 2 including the definition and Security model of CLS. In Section 3, we then review a certificateless short signature scheme, proposed by Choi et al. [5]. Then, we show the cryptanalysis of this scheme and point out the weakness of the security analysis in Section 4. Finally, the conclusions of this paper are given in Section 5.

## 2. Preliminaries.

In this section, we briefly describe the bilinear map at first, and then present the framework and security models of certificateless signatures.

### 2.1. Bilinear map.

A bilinear map is a mapping $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. $\mathbb{G}_1$ and $\mathbb{G}_2$ are additive cyclic groups of prime order $q$, and $\mathbb{G}_T$ is a multiplicative cyclic group of the same order $q$. A bilinear map concerns the following properties:

(1) Computable: given any $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, there exists a polynomial time algorithm to compute $e(P, Q) \in \mathbb{G}_T$.
(2) Bilinear: for any $x, y \in \mathbb{Z}_q^*$, we have $e(xP, yQ) = e(P, Q)^{xy}$ for any $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$.
(3) Non-degenerate: $e(P_1, P_2) \neq 1$ if $P_1$ is a generator of $\mathbb{G}_1$ and $P_2$ is a generator of $\mathbb{G}_2$.

The above is the normal form; however, if $\mathbb{G}_1 = \mathbb{G}_2$, the bilinear map will be denoted by $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ sometimes, where $\mathbb{G}$ is an additive cyclic group of prime order $q$, and $\mathbb{G}_T$ is a multiplicative cyclic group of the same order $q$. In the following we only consider $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$.

2.2. **Certificateless signature (CLS).** A certificateless signature scheme involves three entities, the KGC, a user, and a verifier. Generally, it consists of the following algorithms: Setup, Partial-Private-Key-Extract, Set-Secret-Value, Set-Secret-Key, Set-Public-Key, Sign, and Verify:

- Setup: This algorithm, run by the KGC, takes a security parameter as input, and then returns master-key and system parameter, param.
- Partial-Private-Key-Extract: This algorithm, run by the KGC, takes param, master-key and a user's identity $ID$ as input. It generates a partial-private-key $D_{ID}$, and sends it to the user via a secure channel.
- Set-Secret-Value: This algorithm, run by a user, returns a secret value, $r_{ID}$.
- Set-Secret-Key: This algorithm, run by a user, takes the user's partial-private-key $D_{ID}$ and the secret value $r_{ID}$ as input, then returns the user's full secret key.
- Set-Public-Key: This algorithm, run by a user, takes param and the user's full secret key as input, and returns a public key $pk_{ID}$ for the user.
- Sign: This algorithm, run by a user (signer), takes param, a message $m$, and the user's full secret key as input. It then generates $\sigma$ as the signature for the message $m$.
- Verify: This algorithm, run by a verifier, takes param, a public key $pk_{ID}$, a message $m$, a user's identity $ID$, and a signature $\sigma$ as input. It returns 1 as the verifier accepts $\sigma$ if $\sigma$ is the signature of the message $m$, the public key $pk_{ID}$, and the user with identity $ID$. It returns 0 if not.

2.3. **Security model of CLS.** For security of CLS, there are several adversaries which act as different roles. We usually assume that Type I adversary is an outsider and Type II adversary is the KGC, whereas both of their goals are to generate a forged signature existentially. Nevertheless, Huang et al. [9, 10] categorized the Type I and II adversaries into three levels, referred to as Normal, Strong, and Super adversaries (ordered by their abilities). The Super adversary has been proven to be more powerful than the Strong one without doubt. Accordingly, if a CLS scheme can be secure against the Super, then it can also be secure against the Strong. In other words, if it is insecure against the Strong, it definitely is insecure against the Super. In this paper, we show Game Strong I which simulates the Strong Type I adversary as Huang et al defined [10].[1]

**Game Strong I.** An adversary $\mathcal{A}_I$ interacts with a challenger $\mathcal{C}$ in this game. $\mathcal{A}_I$ acts as an outsider and performs the adaptive chosen message and identity attack. There are three phases in the game: *Setup*, *Attack*, and *Forgery*.

*Setup*: The challenger $\mathcal{C}$ runs Setup and generates *param* to $\mathcal{A}_I$.

*Attack*: $\mathcal{A}_I$ can adaptively submit queries to the following oracles in a polynomial number times.

1. **Create-User**: $\mathcal{A}_I$ can submit $ID$ to this oracle. Nothing will be returned by the oracle if $ID$ has been created before. Otherwise, it will perform Partial-Private-Key-Extract, Set-Secret-Value, and Set-Public-Key for the identity $ID$ to get the partial-private-key $D_{ID}$, the secret value $r_{ID}$, and the public key $pk_{ID}$, thus $ID$ is said to be created and $pk_{ID}$ is returned.

[1] We omit to show Game Normal I modelling the Normal Type I adversary, since these are not used in this paper. However, readers could refer to the paper by Huang et al. [9, 10] for more details.

2. **Public-Key-Replace**: $\mathcal{A}_I$ can submit $(ID, r'_{ID}, pk'_{ID})$ to this oracle for replacing the public key, where $ID$ has been created. The oracle will update the $ID$'s public key/secret value pair. If $ID$ has not been created, no action will be performed.
3. **Secret-Value-Extract**: $\mathcal{A}_I$ can submit $ID$ to this oracle, and then it will return the secret value $r_{ID}$ if $ID$ has been created. Otherwise, returns a symbol $\perp$. Here, $r_{ID}$ is the original secret value and has never been replaced.
4. **Partial-Private-Key-Extract**: $\mathcal{A}_I$ can submit $ID$ to this oracle, and then it returns the partial private key $D_{ID}$ if $ID$ has been created. Otherwise, returns $\perp$.
5. **Strong-Sign**: $\mathcal{A}_I$ can submit $(m, ID, r_{ID})$ to this oracle, where $m$ is the message to be signed. It returns $\perp$ if $ID$ has not been created. Otherwise, it outputs a signature $\sigma$ which satisfies
   $\mathsf{Verify}(\sigma, m, ID, pk_{ID}) = 1$. ($pk_{ID}$ is the current public key of $ID$.)

*Forgery*: Finally, $\mathcal{A}_I$ outputs a forged signature $\sigma^*$ of $(m^*, ID^*, r_{ID^*})$.

For existential forgery, $\mathcal{A}_I$ wins this game if and only if the following conditions hold.

1. $\mathsf{Verify}(\sigma^*, m^*, ID^*, pk_{ID^*}) = 1$.
2. $\mathcal{A}_I$ has never submit $ID^*$ to **Partial-Private-Key-Extract**.
3. $\mathcal{A}_I$ has never submit $(m^*, ID^*, r_{ID^*})$ to **Strong-Sign**.

**Definition 2.1.** *A certificateless signature scheme is provably secure against the Strong Type I adversary if no probabilistic polynomial time adversary wins Game Strong I with non-negligible probability.*

In addition, we also show Game Super I which simulates the Super Type I adversary as Huang et al defined [10].

**Game Super I.** An adversary $\mathcal{A}_I$ interacts with a challenger $\mathcal{C}$ in this game. $\mathcal{A}_I$ acts as an outsider and performs the adaptive chosen message and identity attack. There are three phases in the game: *Setup*, *Attack*, and *Forgery.*

*Setup*: The challenger $\mathcal{C}$ runs $\mathsf{Setup}$ and generates *param* to $\mathcal{A}_I$.

*Attack*: $\mathcal{A}_I$ can adaptively submit queries to the following oracles in a polynomial number times.

1-4. As Game Strong I.

5. **Super-Sign**: $\mathcal{A}_I$ can submit $(m, ID)$ to this oracle, where $m$ is the message to be signed. It returns $\perp$ if $ID$ has not been created. Otherwise, it outputs a signature $\sigma$ which satisfies
   $\mathsf{Verify}(\sigma, m, ID, pk_{ID}) = 1$. ($pk_{ID}$ is the current public key of $ID$.)

*Forgery*: Finally, $\mathcal{A}_I$ outputs a forged signature $\sigma^*$ of $(m^*, ID^*)$.

For existential forgery, $\mathcal{A}_I$ wins this game if and only if the following conditions hold.

1. $\mathsf{Verify}(\sigma^*, m^*, ID^*, pk_{ID^*}) = 1$.
2. $\mathcal{A}_I$ has never submit $ID^*$ to **Partial-Private-Key-Extract**.
3. $\mathcal{A}_I$ has never submit $(m^*, ID^*)$ to **Strong-Sign**.

**Definition 2.2.** *A certificateless signature scheme is provably secure against the Super Type I adversary if no probabilistic polynomial time adversary wins Game Super I with non-negligible probability.*

3. **Review of Choi et al.'s certificateless short signature scheme.** In the literature [10, 13, 15], there exists an open problem where short CLS schemes cannot be secure against the Strong and Super Type I adversaries. Recently, Choi et al. proposed a short CLS scheme and claimed that it is secure against the Super Type I adversary, which implies it solves the open problem. Here in this section, we review the scheme of Choi et al. [5] which is describe as follows.

Setup: Let $\mathbb{G}$ be a cyclic additive group of prime order $q$ with a generator $P$, $\mathbb{G}_T$ be a cyclic multiplicative group of the same order, and a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. In addition, let $H_1, H_1', H_2 : \{0,1\}^* \to \mathbb{G}$ and $\mathcal{H}, \mathcal{H}' : \{0,1\}^* \to \mathbb{Z}_q^*$ be cryptographic hash functions. The KGC randomly chooses $s \in \mathbb{Z}_q^*$ as the master-key and accordingly sets the master-public-key $P_{pub} = sP$. Finally, it returns master-key $= s$ and system parameter param $= \langle \mathbb{G}, \mathbb{G}_T, e, q, P, P_{pub}, H_1, H_1', H_2, \mathcal{H}, \mathcal{H}' \rangle$.

Partial-Private-Key-Extract: Given a user's identity $ID$, the KGC uses master-key and first sets $Q_{ID} = H_1(ID)$ and $\tilde{Q}_{ID} = H_1'(ID)$. It then computes $D_{ID,1} = sQ_{ID}$ and $D_{ID,2} = s\tilde{Q}_{ID}$. Finally, generates a partial-private-key $D_{ID}$ to the user, where $D_{ID} = (D_{ID,1}, D_{ID,2})$.

Set-Secret-Value: The user $ID$ chooses $r_{ID} \in \mathbb{Z}_q^*$ at random, and sets $r_{ID}$ as his secret value.

Set-Secret-Key: This algorithm, run by a user, takes the user's partial-private-key $D_{ID}$ and secret value $r_{ID}$ as input and returns the full secret key $sk_{ID} = (D_{ID}, r_{ID})$.

Set-Public-Key: The user $ID$ takes param, the user's secret value $r_{ID}$ and identity $ID$, and returns $pk_{ID} = r_{ID}P$ as his public key.

Sign: Given a message $m$ and $ID$'s secret key, the signer/user first sets $h = \mathcal{H}(m, ID, pk_{ID})$ and $\tilde{h} = \mathcal{H}'(m, ID, pk_{ID})$, and then returns $\sigma = hD_{ID,1} + \tilde{h}D_{ID,2} + r_{ID}H_2(m, ID, pk_{ID})$ as the signature of $(m, ID, pk_{ID})$.

Verify: To verify a signature $\sigma$ of $(m, ID, , pk_{ID})$, a verifier takes *param*, the public key $pk_{ID}$, the message $m$, the user's identity $ID$, and the signature $\sigma$. He first obtains $h = \mathcal{H}(m, ID, pk_{ID})$, $\tilde{h} = \mathcal{H}'(m, ID, pk_{ID})$, $Q_{ID} = H_1(ID)$, and $\tilde{Q}_{ID} = H_1'(ID)$, and then checks whether the equation, $e(\sigma, P) = e(hQ_{ID} + \tilde{h}\tilde{Q}_{ID}, P_{pub}) \cdot e(pk_{ID}, H_2(m, ID, pk_{ID}))$, holds or not. Return 1 if it holds, and return 0 if not.

For the security analysis, Choi et al. proved this scheme is secure (existentially unforgeable) against the Super Type I adversary, thus it should be secure against Strong Type I adversary as well.

## 4. Cryptanalysis.

**4.1. Breaking Choi et al.'s scheme.** We have found that Choi et al.'s scheme is insecure against the Strong or Super Type I adversary. The cryptanalysis is given as follows, where the Strong Type I adversary can forge a user's signature on any message existentially.

1. Let $\mathcal{A}_I$ be the Strong Type I adversary and $\mathcal{C}$ be the challenger in the Game Strong I. $\mathcal{C}$ passes the system parameter *param* to $\mathcal{A}_I$ and allows $\mathcal{A}_I$ to run.
2. $\mathcal{A}_I$ chooses a secret value, $r'_{ID} \in \mathbb{Z}_q^*$, at random and computes the corresponding public key $pk'_{ID} = r'_{ID}$.
3. $\mathcal{A}_I$ submits $(m_1, ID, pk'_{ID})$ and $(m_2, ID, pk'_{ID})$ to $\mathcal{H}$, $\mathcal{H}'$, and $H_2$ oracles. $\mathcal{C}$ returns the corresponding values, $(h_1, h_2, \tilde{h}_1, \tilde{h}_2, T_1, T_2)$, where $h_1 = \mathcal{H}(m_1, ID, pk'_{ID})$, $h_2 = \mathcal{H}(m_2, ID, pk'_{ID})$, $\tilde{h}_1 = \mathcal{H}(m_1, ID, pk'_{ID})$, $\tilde{h}_2 = \mathcal{H}'(m_2, ID, pk'_{ID})$, $T_1 = H_2(m_1, ID, pk'_{ID})$, and $T_2 = H_2(m_2, ID, pk'_{ID})$.
4. $\mathcal{A}_I$ then queries two signatures of $(m_1, ID, r'_{ID})$ and $(m_2, ID, r'_{ID})$ where $m_1$ and $m_2$ are the messages to be signed, respectively, with the target identity $ID$ and the secret value $r_ID'$. $\mathcal{C}$ then return two valid signatures, $\sigma_1'$ of $(m_1, ID, pk'_{ID})$ and $\sigma_2'$ of $(m_2, ID, pk'_{ID})$ as Eq 1 and 2,

$$\sigma_1' = h_1 D_{ID,1} + \tilde{h}_1 D_{ID,2} + r'_{ID} T_1 \quad (1)$$

$$\sigma_2' = h_2 D_{ID,1} + \tilde{h}_2 D_{ID,2} + r'_{ID} T_2 \quad (2)$$

5. $\mathcal{A}_I$ can obtain the following equations, Eq 3 and 4, due to Eq 1 and 2.

$$\sigma_1' - r_{ID}' T_1 = h_1 D_{ID,1} + \tilde{h}_1 D_{ID,2} \quad (3)$$

$$\sigma_2' - r_{ID}' T_2 = h_2 D_{ID,1} + \tilde{h}_2 D_{ID,2} \quad (4)$$

Since $\sigma_1'$, $\sigma_2'$, $T_1$, $T_2$ and $r_{ID}'$ are known, let $S_1 = \sigma_1' - r_{ID}' T_1$ and $S_2 = \sigma_2' - r_{ID}' T_2$. $\mathcal{A}_I$ can straightly have Eq 5 and 6.

$$S_1 = h_1 D_{ID,1} + \tilde{h}_1 D_{ID,2} \quad (5)$$

$$S_2 = h_2 D_{ID,1} + \tilde{h}_2 D_{ID,2} \quad (6)$$

$\mathcal{A}_I$ thus has Eq 7 and 8, then gets Eq 9 as a result.

$$h_1^{-1}(S_1) = D_{ID,1} + h_1^{-1}\tilde{h}_1 D_{ID,2} \quad (7)$$

$$h_2^{-1}(S_2) = D_{ID,1} + h_2^{-1}\tilde{h}_2 D_{ID,2} \quad (8)$$

$$h_1^{-1}(S_1) - h_2^{-1}(S_2) = (h_1^{-1}\tilde{h}_1 - h_2^{-1}\tilde{h}_2)\tilde{D}_{ID} \quad (9)$$

Eventually, $\mathcal{A}_I$ obtains $D_{ID,2}$ by computing $D_{ID,2} = (h_1^{-1}\tilde{h}_1 - h_2^{-1}\tilde{h}_2)^{-1}(h_1^{-1}S_1 - h_2^{-1}S_2)$, and $\mathcal{A}_I$ also can obtain $D_{ID,1}$ by using $D_{ID,2}$. Upon getting the partial-private-key $D_{ID} = (D_{ID,1}, D_{ID,2})$, $\mathcal{A}_I$ can forge valid signatures on whatever messages as he wants on behalf of the target user with identity $ID$. Consequently, $\mathcal{A}_I$ breaks the existential unforgeability of Choi et al.'s scheme.

On the other hand, the Strong Type I adversary can submit the target $ID^*$ to obtain the secret value at first with other steps as before, and finally $\mathcal{A}_I$ also can have partial-private-key. We conclude that Choi et al.'s scheme suffers from the above attack in Game Strong I, which means the scheme is insecure against the Super Type I adversary. In fact, the above attack strategy is an extension of Shim's attack [13].

4.2. **Discussions for the security proof of Choi et al.'s scheme.** A CLS scheme is provably secure under the security model, which implies that the adversary, simulated by the security game, has no polynomial time algorithm to win the game with non-negligible probability. Therefore, any scheme with security proof given but later be found insecure under the security model implies that the provided security proof is incorrect. Analysis these incorrect proofs is meaningful and useful since these information can support our attack on one hand and can also give us ideas on how to improve the security of those schemes theoretically. Regarding the security proof of Choi et al.'s scheme, please refer to [5] for details. We analyze and present the a few weaknesses with respect to the proof of Choi et al. as follows. Here we assume the forged signature $\sigma^*$ is valid on $(m^*, ID^*)$.

(1) $\mathcal{H}$ and $\mathcal{H}'$ are not random oracles. The outputs of $\mathcal{H}$ and $\mathcal{H}'$ oracles are dependent, which means the outputs of $\mathcal{H}$ will influence on those of $\mathcal{H}'$.

(2) Formally, for provable security, a signature scheme is said to be $(t, \epsilon, q_S)$-secure if and only if it is existentially unforgeable, where $t$ is the running time, $\epsilon$ is the advantage (ie., probability) of winning the security game, and $q_S$ is the maximum number of times an attacker can query the signature oracle, which are usually sufficiently large for a secure scheme. However, by tracing the security proof, we found that Choi et al.'s scheme is proven to be $(t, \epsilon, 1)$-secure which means that it is only allowed any attacker to query the signature oracle once. In other words, when an attacker queries the signature oracle over once and gets at least two different signatures, then he can always break the existential unforgeability of Choi et al.'s scheme.

On the other hand, there exists another Type I adversary, presented by Tso et al. [15], which is not the Strong and Super Type I defined by Huang et al. [9, 10] and is a little weaker than Super Type I. However, we have found Choi et al.'s scheme is also insecure against this new kind of Type I adversaries. We there conclude that Choi et al.'s scheme is only secure against the Normal Type I adversary, but not against higher ones.

5. **Conclusions.** To overcome the key escrow problem of ID-based systems, certificateless cryptography has drawn the attention of the research community in the last few years. In particular, lots of certificateless signature schemes have been presented in the literature. Recently, Choi et al. proposed an efficient certificateless short signature scheme, and claimed that their scheme reaches the strongest security level. However, it has been broken in this paper. We demonstrate that their scheme is insecure against the Strong Type I adversary. Finally, we show the incorrectness of security proof of this scheme.

**Acknowledgement.** This related research was partially supported by the National Science Council of the Republic of China, Nos. NSC101-2221-E-005-083 and NSC101-2628-E-004-01-MY2.

## REFERENCES


[1] S. S. Al-Riyami, and K. G. Paterson, *Certificateless public key cryptography*, LNCS 2894, springer, pp. 452-473, 2003.

[2] D. Boneh, and X. Boyen, *Short signatures without random oracles*, LNCS 3027, springer, pp. 56-73, 2004.

[3] Y. C. Chen, C. L. Liu, G. Horng, and K. C. Chen, A provably secure certificateless proxy signature scheme, *International Journal of Innovative Computing, Information and Control Control*, vol. 7, no. 9, pp. 5557-5569, 2011.

[4] K. Choi, J. Park, J. Hwang, and D. Lee, *Efficient certificateless signature schemes*, LNCS 4521, springer, pp. 443-458, 2007.

[5] K. Choi, J. Park, and D. Lee, A new provably secure certificateless short signature scheme, *Journal of Computers & Mathematics with Applications*, vol. 61, no. 7, pp. 1760-1768, 2011.

[6] H. Du, and Q. Wen, Efficient and provably-secure certificateless short signature scheme from bilinear pairings,*Journal of Computers Standards & Interfaces*, vol. 31, no. 2, pp. 390-394, 2009.

[7] C. I. Fan, R. H. Hsu, and P. H. Ho, Truly non-repudiation certificateless short signature scheme from bilinear pairings,*Journal of information science and engineering*, vol. 27, no. 3, pp. 969-982, 2011.

[8] B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng, Certificateless signature: a new security model and an improved generic construction, *Journal of Designs, Codes and Cryptography*, vol. 42, no. 2, pp. 109-126, 2007.

[9] X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, *Certificateless signature revisited*, LNCS 4586, springer, pp. 308-322, 2007.

[10] X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, Certificateless signatures: new schemes and security models, *Journal of Computer journal*, vol. 55, no. 4, pp. 457-474, 2012.

[11] D. Jao, and K. Yoshida, *Boneh-boyen signatures and the strong diffie-hellman problem*, LNCS 5671, springer, pp. 1-16, 2009.

[12] A. Shamir, *Identity based cryptosystems and signature schemes*, LNCS 196, springer, pp. 47-53, 1984.

[13] K. Shim, Breaking the short certificateless signature scheme, *Journal of Information Sciences: an International Journal*, vol. 179, no. 3, pp. 303-306, 2009.

[14] M. Tian, L. Huang, and W. Yang, On the security of a certificateless short signature scheme, *Cryptology ePrint Archive 2011/419*, available at http://eprint.iacr.org/2011/419.pdf.

[15] R. Tso, X. Huang, and W. Susilo, Strongly secure certificateless short signatures, *Journal of Systems and Software*, vol. 85, no. 6, pp. 1409-1417, 2012.

[16] R. Tso, X. Yi, and X. Huang, Efficient and short certificateless signatures secure against realistic adversaries, *Journal of The Journal of Supercomputing*, vol. 55, no. 2, pp. 173-191, 2011.

[17] T. Y. Wu, T. T. Tsai, Y. M. Tseng, Revocable ID-based signcryption scheme, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 3, no. 3, pp. 240-251, 2012.

[18] D. H. Yum, and P. J. Lee, *Generic construction of certificateless signature*, LNCS 3108, springer, pp. 200-211, 2004.